UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/649,097	08/28/2000	Hisashi Ishikura	Q60517	7802

7590 03/23/2004

Sughrue Mion Zinn Macpeak & Seas
2100 Pennsylvania Avenue NW
Washington, DC 20037

EXAMINER	
NGUYEN, NAM V	
ART UNIT	**PAPER NUMBER**
2635	

DATE MAILED: 03/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/649,097	ISHIKURA ET AL.	
	Examiner	Art Unit	
	Nam V Nguyen	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,8-14 and 17-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,8-14 and 17-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This communication is in response to applicant's response to amendment B which is filed October 10, 2003 by a request for continued examination.

An amendment to the claims 1-2, 6-7 and 15-16 have been entered and made of record in the application of Ishikura et al. for a "vehicle key system" filed August 28, 2000.

Claims 2, 6-7 and 15-16 are cancelled.

Claims 1, 3-5, 8-14 and 17-19 are pending.

Response to Arguments

Applicant's amendments and argument to the rejected claims are insufficient to distinguish the claimed invention from the cited prior arts or overcome the rejection of said claims under 35 U.S.C § 103(a) as discussed below. Applicant's amendment and argument with respect to the pending claims 1, 3-5 8-14 and 17-19, filed October 10, 2003, have been fully considered but they are not persuasive for at least the following reasons.

On page 9, fourth paragraph, Applicant agrument that Flick in view of Scott failed to teach or suggest all the limitations of the vehicle system of claim 1. The Claims in a pending application should be given their broadest reasonable interpretation. In re Pearson, 181 USPQ 641 (CCPA 1974). Flick discloses a biometric sensor may be positioned at the vehicle or be carried by a handheld remote transmitter, for example. The biometric characteristic sensor may

be one of a fingerprint sensor, a voice pattern sensor, a facial pattern sensor, a skin pattern sensor, a venous pattern sensor, a hand sensor, or a retinal scanner, for example. The biometric characteristic learning means may be switchable between a learning mode permitting learning of at least the biometric characteristic of an individual, and a secure mode. In one embodiment, the biometric characteristic learning means may include biometric characteristic deleting means for deleting all prior learned individuals based upon entering the learning mode. The biometric characteristic verifying means may further include learning mode entered indicating means for indicating that the learning mode has been entered. The learning mode entered indicating means may comprise time lapse means for indicating when the learning mode has last been entered. The time lapse means, in turn, may comprise means for progressively indicating a passage of time since the learning mode has last been entered. Alternately, the biometric characteristic verifying means may include learned individual number indicating means for indicating a number of learned individuals. The biometric characteristic verifying means may also alternately include learned individual change indicating means for indicating a change in a number of learned individuals or means for generating an indication relating to whether a new individual has been learned by the learning means. The verifying means may further comprise activating means for causing the indicating means to generate an indication (column 2 line 43 to column 3 line 6; see Figures 3-6). Flick further discloses said verification means comprising feature verification means for verifying the features extracted from the finger print information received from said transmitter against features on an authorized user stored by said receiver (column 8 lines 55 to 66; see Figure 5) and comprehesively determining means for determining whether or not a user manipulating said transmitter is an authorized user and whether or not the manipulation is

directed toward the vehicle corresponding to said transmitter (column 8 line 66 to column 9 line 8; column 9 lines 20 to 35). Flick also teaches that a method for increasing security in permitting remote control of a function associated with a vehicle and using at least one uniquely coded remote transmitter 50, and a receiver 13 within the vehicle for receiving a signal from the uniquely coded remote transmitter. The method preferably comprises the steps of: storing in a memory 14 a unique code of a remote transmitter 50 to define a learned remote transmitter capable of causing performance of a function associated with the vehicle, and generating an indication relating to whether a new uniquely coded remote transmitter has been stored in the memory to thereby alert the user of a potentially unauthorized learned remote transmitter capable of remotely performing the function associated with the vehicle (column 9 lines 20 to 35). One skilled in the art understands that the vehicle security system verifies a biometric characteristic and a unique code of a remote transmitter.

Scott et al. disclose a personal identification device including an identifier storage memory for storing an ID code specific to said transmitter (column 5 lines 16 to 26; column 6 lines 54 to 61; see Figures 1-2 and 8) in order to associate an ID code with the remote controlled device when verifying for permission to configure the automotive remote key entry system.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to have a transmitter including an identifier store in a memory of Scott et al. with the biometric characteristic of Flick with the motivation for doing so would have been to increase the security of the portable remote control identification vehicle system in order to avoid unauthorized users.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flick (US# 6,140,939) and in view of Scott et al. (US# 6,484,260).

Referring to claim 1, Flick discloses a vehicle key system for verifying identity of fingerprint information about a user's fingerprint and for controlling pieces of equipment in a vehicle according to a verification result (column 2 lines 16 to 21; see Figure 3), said system comprising:

A transmitter (50) (i.e. a remote transmitter) including a fingerprint information capturing means (59) (i.e. a biometric sensor) for capturing fingerprint information from a user's fingerprint (column 2 lines 42 to 48; column 5 lines 5 to 13; see Figure 2), and a transmitting means (57) (i.e. a transceiver circuit) for transmitting only the fingerprint information (i.e. fingerprint characteristic) captured by said fingerprint information capturing means (59) (i.e. biometric sensor) (column 8 line 26 to column 9 line 3; see Figure 5); and

A receiver (13) (i.e. a transceiver) disposed in the vehicle (10) (i.e. vehicle security system), including a receiving means (13a) for receiving the fingerprint information transmitted

from said transmitting means (57a) of said transmitter (50) (column 8 line 26 to column 9 line 3; see Figures 1 and 5),

a verification means (49 or 82) for verifying the received fingerprint information against a list of pieces of previously stored fingerprint information (column 6 lines 40 to 64; column 8 line 19 to column 9 line 3; see Figure 5), said verification means (49 or 82) including feature verification means for verifying the features extracted from the fingerprint information received from said transmitter (50) against features of an authorized user stored by said receiver; an identifier verification means for verifying the specific identifier received from said transmitter (50) and the specific identifier stored by said receiver (column 8 lines 55 to 66; column 9 lines 21 to 35), and comprehensively determining means for determining whether or not a user manipulating said transmitter (50) is an authorized user and whether or not the manipulation is directed toward the vehicle corresponding to said transmitter (column 8 line 66 to column 9 line 8; column 9 lines 20 to 35); and

a control means (86) (i.e. vehicle remote start controller) for controlling said pieces of equipment (30-37 and 41-46; see Figures 1 and 5) in the vehicle according to verification results from said verification means (column 9 lines 9 to 19).

However, Flick did not explicitly disclose that a transmitter including an identifier storage means for storing an identifier specific to said transmitter. Flick discloses that the transmitter transmits a uniquely coded transponder to the vehicle security systems to operate vehicle control system in prior art (column 1 lines 46 to 55; column 2 lines 3 to 13).

In the same field of endeavor of remote control identification system, Scott et al. disclose that a transmitter (6) (i.e. personal identification device) including an identifier storage means

(20) (i.e. memory) for storing an identifier (i.e. an ID code) specific to said transmitter (6) and fingerprint template (column 5 lines 16 to 26; column 6 lines 54 to 61; column 8 lines 30 to 39; see Figures 1-2 and 8) in order to associate an ID code with the remote controlled device when verifying for permission to configure the automotive remote key entry system to increase security.

One of ordinary skilled in the art recognizes the need to have a transmitter including an identification codes store in a memory of Scott et al. in using at least one uniquely coded remote transmitter of Flick because Flick suggests it is desired to provide a remote transmitter with at least one uniquely coded stored in a memory and additional biometric characteristic sensor to read and learn a fingerprint would prevent thief of valuables from a vehicle (column 1 line 65 to column 2 lines 14) and a receiver within the vehicle for receiving a signal from the uniquely coded remote transmitter to permit remote control of a function associated with a vehicle (column 9 lines 20 to 35) and Scott et al. teach that a transmitter including an identifier storage means for storing an identifier specific to said transmitter (column 6 lines 54 to 61) in order to verify that the ID code of the transmitter matches the stored ID code of a secure automobile system. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention was made to have a transmitter including an identification codes store in a memory of Scott et al. in using at least one uniquely coded remote transmitter of Flick with the motivation for doing so would have been to provide a remote control transmitter has a plurality of verification function to increase security in order to avoid unauthorized users to access to a vehicle control system.

Referring to claim 3, Flick in view of Scott et al. disclose a vehicle key system according to claim 1, Flick discloses wherein said control means comprising engine control means (86) (i.e. vehicle remote start controller) for controlling an engine according to the verification result from said receiver (85) (column 8 lines 55 to 66; see Figure 5), door control means (11) for controlling a lock of doors according to the verification results from said receiver (see Figure 4) (column 8 lines 26 to 45), and a trunk control means (25) for controlling a lock of a trunk according to the verification result of the receiver (see Figure 3) (column 4 lines 53 to 60; column 8 lines 1 to 18).

Claims 4-5, 8-14 and 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flick (US# 6,140,939) and in view of Scott et al. (US# 6,484,260) as applied to claim 1, and further view of Hsu et al. (US# 6,100,811).

Referring to claim 4, Flick in view of Scott et al. disclose a vehicle key system according to claim 1, Flick discloses wherein said receiver further comprising:

A first operation means (52a-52d) (i.e. input selection switches) for selecting only armed or disarmed modes to a manipulation performed by a user (column 5 lines 5 to 39; see Figure 2),

A first verification data-selection state storage means (i.e. memory in CPU) for storing the verification data-selection state (i.e. input interface of switches) indicating a selection state of the verification data whose value is set by said first operation means (52a-52d) and a selection state of the verification data received by said transmitter (50) (i.e. remote transmitter) (column 4 lines 47 to 52; column 5 lines 14 to 55), and

A display means (58) for displaying which information to be verified is selected from the fingerprint information or the identifier selected (column 5 line 63 to column 6 line 2).

However, Flick in view of Scott et al. did not explicitly disclose that selecting only the fingerprint information, only the identifier or the both of them according to a manipulation performed by a user.

In the same field of endeavor of remote control vehicle system, Hsu et al. disclose that selecting only the fingerprint information, only the identifier or the both of them according to a manipulation performed by a user (column 2 lines 25 to 47; column 7 lines 27 to 48; see Figure 7) in order to control the operational modes of the remote control system.

At the time the invention, it would have been obvious to a person of ordinary skill in the art to recognize the need for changing the selecting modes of the fingerprint information, only the identifier or combination of both in the switching the controller between armed or disarmed modes of operation of Flick in view of Scott et al. because selecting the modes of the fingerprint information result would improve the reliable and convenient operation of the transmitter that has been shown to be desirable in the vehicle security system of Flick in view of Scott et al.

Referring to claim 5, Flick in view of Scott et al. and further view of Hsu et al. disclose a vehicle key system according to claim 4, Flick discloses wherein said transmitter (10) further comprising:

A second operation means (20-29) for selecting operational function according to a manipulation performed by a user (column 4 lines 31 to 60; see Figure 1), and

A second verification data-selection state storage means (14) for storing the verification data-selection state indicating a selection state of the verification data (49) whose value is set by said first operation means (52a-52d) and a selection state of the verification data received by said transmitter (50) (column 4 lines 61 to column 5 lines 42; see Figures 1-2).

Referring to claim 8, Flick in view of Scott et al. and further view of Hsu et al. disclose a vehicle key system according to claim 4, Flick discloses wherein an operation unit (30) intended for operating a piece of equipment disposed in said vehicle also serves as said first operation means (30-37 and 41 to 46) (column 5 lines 14 to 32; see Figure 1).

Referring to claim 9, Flick in view of Scott et al. and further view of Hsu et al. disclose a vehicle key system according to claim 8, Flick discloses wherein said equipment (21) (i.e. the sensors of the vehicle) is a navigation device (i.e. movement of the vehicle) (column 1 lines 19 to 30).

Referring to claim 10, Flick in view of Scott et al. and further view of Hsu et al. disclose a vehicle key system according to claim 4, Flick discloses wherein a pedal (20) disposed in said vehicle also serves as said first operation means (column 4 lines 53 to 60; see Figure 1).

Referring to claims 11-14 and 17-19, Flick in view of Scott et al. and further view of Hsu et al. disclose a vehicle key system according to claims 2-5 and 8-10, Hsu et al. discloses wherein if said verification means (30) (i.e. matching device and check ID) previously stores no

fingerprint information (i.e. guest mode), when the received information includes the system-specification identifier (i.e. a secret combination), said verification means performs only the verification of the received identifier against a previously stored identifier (column 2 lines 34 to 47; column3 lines 28 to 37; column 7 lines 27 to 48; see Figure 7).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nam V Nguyen whose telephone number is 703-305-3867. The examiner can normally be reached on Mon-Fri, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on 703-305-4704. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9314 for regular communications and 703-872-9314 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Nam Nguyen
March 18, 2004

MICHAEL HORABIK
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600